SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Part of ICETE 2014 - 11th International Joint Conference on e-Business and Telecommunications, 2014, pages 411-416

Experimental study of performance and security constraints on wireless key distribution using random phase of multipath radio signal

Sulimov A., Smolyakov A., Karpov A., Sherstyukov O.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

The paper presents the results of experimental distribution of encryption keys based on random carrier phase of fading radio signal measured in a multipath environment. The random bits extraction scheme was proposed and tested in practice. The proposed scheme is universal and applicable to measurements digitizing of any observable random variable. Experimental study of spatial correlation of multipath signal phase in the case of transverse spatial diversity is carried out. Experimental estimation of the key generation rate and the probability of its passive interception at different distances between the legal user and potential eavesdropper are also performed. It is shown that the parameters of bit extraction procedure significantly affect on the performance and security of the key distribution process.

Keywords

Channel reciprocity, Common randomness, Encryption keys distribution, Key interception, Multipath radio propagation, Randomness of carrier phase, Rate of encryption key distribution, Spatial correlation